Contents

List of Figures

Abstract

This research aims to explore one very promiment and potential application for the blockchain, which is a decentralized electronic voting system, by creating a minimum viable decentralized voting application, capable of launching an election, casting votes and displaying results, all while ensuring transaprency, anonymity, security and above all the correctness of the results.

Keywords: Decentralized Electronic Voting System, Voting, Blockchain

Chapter 1

Introduction

1.1 Background

As the hype surrounding bitcoin is slowly waning, the industry is becoming more and more interested in its underlying technology: the blockchain. Now, proponents claim blockchain technology to be one of the most important new technologies of our time, about to take society by storm, and bitcoin served as the first, most thorough and complete proof of concept. In fact, Marc Andreessen, founder of VC firm Andreessen Horowitz and one of the most influential members of Silicon Valley, claimed in a New York Times article that the invention of the blockchain is as important and influential as the creation of the Internet itself[6].

Along with assets registry, secure sharing of medical data and supply chain and logistics monitoring, electronic voting is one of the most prominent potential applications for the surging blockchain technology.

1.2 Key Concepts

1.2.1 Voting

According to Oxford English dictionary, voting is *"a formal indication of a choice between two or more candidates or courses of action, expressed typically through a ballot or a show of hands"*, and the very first forms of voting date back to approximately 508 B.C in ancient Greece where the earliest form of democracy was implemented[5]. Greeks had a "negative" election – that is, each year voters, who were the male landowners, were asked to vote for the political leader or "candidates" they most wanted to be exiled for the next ten years.

The early ballot system was voters wrote their choice on broken pieces of pots, ostraka in Greek, and from this name comes our present word to ostracize. If any "candidate" received more than 6,000 votes then the one with the largest number was exiled. If no politician received 6,000 votes then they all remained. Since voters were only male landowners, the number of voters was small. If there was a fairly even spread of votes, no one would be exiled, so usually, only very unpopular political leaders were ostracized or exiled.

The election is the backbone of modern democratic societies, it often takes place at a polling station; it is voluntary in some countries, compulsory in others, such as Australia.

1.2.2 Blockchain technology

Blockchain is a distributed database that maintains a secure and ever-growing ledger of records (known as blocks), allowing for the creation of a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across an entire network of computers.

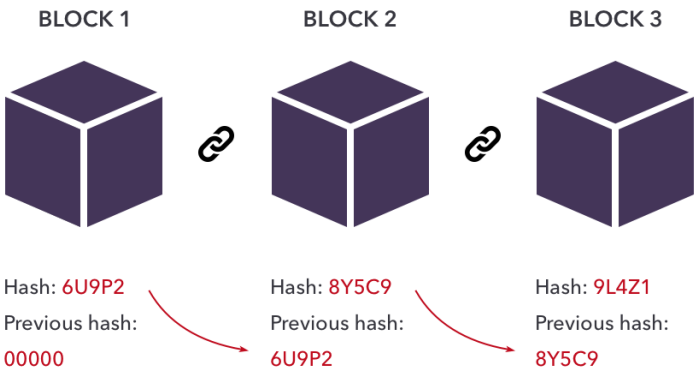

Figure 1.1: Abstract Blockchain blocks visualization

A blockchain network can track orders, payments, accounts, production and much more. And because members of the network share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

1.3 Problem & motivation

Elections are expensive, complicated to set up and even on extreme cases fraudulent, this democratic system is almost 3000 years old and it has not evolved since ancient Greece. It entails an obligation for the voters to rely on third party officials and groups to safely collect votes and publish results, In the case of the modern democratic nation of France for example, there are only 3000 magistrates delegated to supervise and monitor more than 35 000 communes[1], a feat that is inconceivable for them to physically achieve, so setting the human malice apart still leaves room for human error, both leading to the voters carrying justifiable suspicions to any result the ballot may yield. Classic elections also carry hefty financial burdens, the 43rd general election (December 31st, 2020) of Canada had a total estimated cost of $502.4 million[4], the equivalent of the cost of building 5 new hospitals, including administrative areas, operating and emergency rooms, and space for 120 beds[2].

Then comes technology, the premise held while entering various fields is that it will increase efficiency, cut costs and leave all parties involved satisfied, with an abundance of examples of when technology did also keep that premise, voting seems to be a logical place to land in next. Electronic voting systems and semi-electronic ones existed for quite some time, from punched card systems (see figure 1.2) to modern-day digital voting machines. However, they only served to optimize the physical act of punching a card or putting a piece of enveloped paper in a box, although that did cut some costs, may be made the experience of voting more pleasant, but it introduced more security concerns and most importantly it did not solve the essential problem of eliminating third parties, because people still had to trust the hardware and software engineers that programmed the machines to cast the votes, and the servers to not allow for any tampering with the data. People must have faith in not only these people's integrity but also competence.

Figure 1.2: The Votomatic vote recorder, a punch card voting machine originally developed in the mid 1960s

1.4 Purpose & delimitations

The goal of this research is to investigate the possibility of using the new surging blockchain technology as the underlying technology powering an electronic voting system, offering the ability to store the results in a decentralized ledger that should grant the solution attributes like immutability and transparency. We intend to achieve our goal by designing a decentralized e-voting system as a proof-of-concept, capable of launching an election, casting votes, and displaying results, all while ensuring transparency, anonymity, security and above all correctness of the results. It is of major importance to define the scope of this research document and its underlying implementation. First, the implementation of the proof of concept is not by any means complete and thorough but instead functionality was compromised in favor of delivering an actual election on the blockchain.

Second, regarding blockchain technology, this document will not dive deep into the inner working of the technology, topics like hash functions, cryptography and proof of work mechanism will not be presented in a manner that debates their efficiency since we judge the scientific literature on these manners is of abundance, the focus will instead fall on how the application of this technology on voting would look like. Also as Asaf Ashkenazi said *"Every device and system is hackable—it's just a matter of time and hacker motivation."*[3] so our focus will not fall on defending the robustness of our implementation or any future implementation but rather it will fall on highlighting the promise that this technology presents in terms of robustness. Lastly, code snippets that are unique to this project are included.

Figure 1.3: Proof-of-concept "Verum" Logo

1.5 Document structure

This document is presented in 4 chapters, starting with the introductory chapter in which we will present the reader with a bit of background of the topic and then delve into formally defining the problem we intend to tackle, followed by a brief description of what lies beyond the scope of this research.

In the second chapter, the reader will be presented with sufficient technical background about the two major fields involved in making this project come to life, being the Ethereum blockchain and Web applications. The next chapter will be about the implementation of our proof-of-concept, a chapter in which tools will be introduced and results will be exposed using diagrams, screenshots, and plain old language.

Finally, in the fourth and last chapter, the results and insights gained through the journey of making our proof-of-concept will be discussed, few conclusions drawn and perspectives on what could be enhanced moving forward with this project.

Bibliography

[1] Article LO274 - Code électoral - Légifrance. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006353645.

[2] Cost to Build a Hospital | Hospital Construction Cost. https://www.fixr.com/costs/build-hospital.

[3] Cybersecurity Expert Warns of Increasing Vulnerabilities in Devices | Observer. https://observer.com/2019/09/cybersecurity-expert-asaf-ashkenazi-device-vulnerability-hacking/.

[4] Estimated Cost of the 43rd General Election – Elections Canada. https://www.elections.ca/content.aspx?section=res&dir=rep/off/cou&document=index43&la

[5] History Of Elections. https://www.duvalelections.com/General-Information/Learn-About-Elections/History-Of-Elections.

[6] Marc Andreessen. Why Bitcoin Matters. https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/, 1390323270.